

EXHIBIT 4

Giving Away Our Data for Free is a Market Failure



By convincing users to give away their data for free, digital platforms have caused a market failure. This failure benefits them and harms us, their users. A recent paper explores different ways to fix this.

Digital platforms, such as Google and Facebook, voraciously collect personal information from their users. This information spans many aspects of users' lives, such as location, interests, activities, political opinions, and social interactions. Personal information is collected without compensation to the user, other than providing free internet search by Google or free social networking services by Facebook. Users opt-in by default, providing their personal information to digital platforms that impose a take-it-or-leave-it requirement contract.

There are clearly two markets here: the “primary” market for digital services:
(A) search in the case of Google, social networking service in the case of Facebook; and
(B) the market for the sale of personal information. In a competitive world, these markets would function separately from each other.

Under competition, in market A, prices for internet search or for social network service would be determined by competitive conditions. In market B, users would be able to sell their personal information if they so wished but could also choose not to do so.

The ability of the digital platforms to drive users to accept their take-it-or-leave-it opt-in contract to provide personal data at zero price is a direct result of their market dominance. The collection of data in this fashion enhances the dominant position of the platforms in their respective primary markets and reinforces their ability to collect even more personal data.

In the competitive world, users by default would opt-out from the market for sale of personal information. If a user wanted to enter this market, she would opt-in, sell her personal information and

get compensated by the digital platform. Compensation would depend on the value of the information of a particular user to the platform. A user would accept the offer and participate in market B if the monetary compensation exceeds her value of the loss of privacy implied by the transaction.

Users vary widely on the value they place on privacy and in the value of their personal information to the platforms. Therefore, in a competitive market for personal information, some users would participate, and others would not. Transaction prices for the sale of personal information would also vary and likely be individually negotiated between the platform and the user.

In contrast, at present we observe a *market failure* where all transactions occur at the same zero price, and some transactions that would have occurred under competition do not occur. The market failure is a direct result of the imposition of the take-it-or-leave-it contract by dominant digital platforms and the default opt-in.

"The market failure is a direct result of the imposition of the take-it-or-leave-it contract by dominant digital platforms and the default opt-in."

A digital platform can benefit from this market failure in at least three ways: First, it collects and appropriates data directly from the user and combines it with other data it buys from third parties, such as health or credit card transactions data, as well as public census income and race data, to create a profile that is highly desirable to an advertiser or a political campaign and can be sold at a high price. The appropriation of personal information improves the quality of profiles sold to advertisers and enhances the digital platform's market position in advertising.

Second, data has network effects that improve the quality of the primary services of the platforms. Thus, the appropriation of more personal information enhances the dominance of Google and Facebook in their respective primary markets for internet search and social networking.

Third, the platform does not pay for personal data except by a payment in kind with a service that has a negligible incremental cost. Thus, the platform always benefits from the appropriation of data in exchange for its service, even when the data has small benefits in increasing the quality of the user profile sold to advertisers or small network effects in other services sold by the platform. Most importantly, the platform avoids monetary payments that would be the norm in the but for world and enhances its dominance in its primary market.

There are several harms to users and competition resulting from the requirement contract and the market failure. First, the market failure harms users who would be willing to pay for the primary service of the platform but are not willing to sell their personal information to the platform at zero price and therefore presently do not participate in market B. Second, some of the users participating in the market at zero price would be compensated at a positive price under competition. Third, the market failure, through the acquisition of data, enhances the dominant position of digital platforms in their respective primary market. Fourth, the enhancement of the dominant position in the primary market allows platforms to make more users accept the requirement contract, thereby increasing the group of users who accept the requirement contract and the harm to them.

Users are also harmed because of asymmetric information. They do not know the value of their data to advertisers and/or the digital platforms that harvest them as they have no information of its value in digital platform's transactions with advertisers and infomediaries on the other side of the platform. Additionally, users may underestimate the value of their privacy or this value may increase over time in the perception of the user.

There is also the risk that the mode of competition and innovation in the industry will be frozen at a suboptimal equilibrium from the perspective of data protection since the implemented data extraction strategies may generate superior levels of profitability for the platforms that manage to harvest most of

the personal data, leading to increasing returns to scale and learning-by-doing, resulting in long term dominance.

Remedies that fully reverse the anticompetitive effects are difficult to find because of the multitude of the effects and the long-term dominance they cemented.

A required first remedy is to make “opt-out” the default regime in the collection of personal information, and sellers would opt-in if they so wish. The EU has adopted the opt-out regime in the GDPR based on an approach of “rights” rather than antitrust. But this is hardly enough because of the asymmetrical bargaining power between the user and a dominant digital platform that can act as a monopsonist utilizing significant user-specific information.

“A required first remedy is to make “opt-out” the default regime in the collection of personal information, and sellers would opt-in if they so wish.”

Structural remedies could include (i) a horizontal break-up of the platform (for example Google to Google1, Google2, etc. that start as identical companies) to enhance inter-platform competition; (ii) a rollback of previous mergers, for example with Facebook spinning off Instagram and WhatsApp; and/or (iii) vertical separation by prohibiting the platform to do business in vertically related markets, for example Google spinning off its online travel agency business.

Separation need not be structural; it may be a data separation policy or a data-use break-up. It need not focus only on the dominant platform and the companies controlled by it but may also expand to a partial break up of their third-party ecosystem. Some “light-touch” separation may be achieved by policies that require digital platforms not to use personal data that has been harvested from members of their ecosystems unless they have the explicit consent of these members for the envisaged use. This may break the continuity of the data resources the platform commands as part of the economic entities it controls from the data resources that are provided to it by its third-party ecosystem. “Data separation” policies may be implemented more easily than structural break-ups and could serve to reduce the data advantage that some platforms have in view of the time people spend online and on/ in/ within each platform’s ecosystem.

Another remedy could involve platforms ensuring that even after acquisition, policies at acquired companies that are more protective to privacy of personal data remain in place and are not replaced by the less privacy-oriented policies.

Platforms could switch to a regime of paying users for their data as we outlined earlier, which could lead to the emergence of a non-exclusive licensing market for user data when users opt-in to sharing their data with specific platforms. This would enable users to port their data to the platforms that offer them higher levels of return and better conditions in terms of valuing their privacy.

Non-exclusive licensing could be instituted through a licensing agency that would collect the data from each user and distribute it to platforms. The user would be paid the combined sum of all the amounts that the relevant companies are willing to pay. To determine the “fair” value, one would need to refer to the value of the data in a competitive market. However, this is not currently possible as there is no competitive market, and network effects ensure that a competitive market will not have egalitarian market shares. Digital platforms are likely to exercise their buying power, resulting in downward pricing pressure in the market for personal data depriving the users from a portion of their revenues. A possible solution would be for competition authorities to facilitate users collectively bargaining.

Data portability, providing users with the ability to export their social graph or their search history, constitutes another competition law remedy tackling the problem of the absence of a market for personal data. This ability ensures the free flow of personal data and ensures that users are not captive to a limited number of digital platforms.

The constitution of a “data commons” may also facilitate new entry into data-related markets and, therefore, should be promoted. This may be done by, for instance, enabling the diffusion of data that has been harvested by government bodies. Another option would be to promote the development of “data clubs” that operate on an open, non-exclusive basis and different companies to pool and share data, again respecting high privacy standards. Such data clubs would have to be properly scrutinized to prevent them from serving as facilitators for cartel activity limiting the protection of privacy.

Interoperability remedies may also help to intensify inter-platform competition, thus also contributing to a better protection of privacy-related competition. For instance, as a remedy, Facebook could change from a closed to an open communication network by adopting an open API for user messages, chats, posts, and other communications. This would enable its users to send messages to users of other social networks and could unlock privacy-related competition between Facebook and other social networks, by eroding the number and identity of users’ barrier to entry of Facebook. This barrier may lock in users who value their privacy but have no alternative competitive platform to switch to while preserving the possibility of communicating with their existing social network. Similarly, Google could open APIs that would allow users to submit queries simultaneously in multiple browsers as was the case in the early days of the Internet.

We discuss these issues in more detail at Nicholas Economides and Ioannis Lianos—[Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective](#), forthcoming in the Journal of Competition Law and Economics; and Nicholas Economides and Ioannis Lianos—[Antitrust and Restrictions on Privacy in the Digital Economy](#), Concurrences Review No. 2-2020, pp. 22-30, May 2020.

No related posts.